XSEDE Capability Delivery Plan
UCCAN-6 and UCCAN-9 Identity Management
Last revised 2016-06-01

Background

Use cases describe community needs, requirements, and recommendations for improvements to cyberinfrastructure “CI” resources and services. Engineers analyze use cases to identify which aspects are supported by production components and which constitute gaps in functionality. A Capability Delivery Plan (CDP) is an executive summary of use case support gaps and plans to fill those gaps with new or enhanced capabilities.

Use Case Summary

Use cases CAN-6 (“Canonical 6”) and CAN-9 (“Canonical 9”) describe how the XSEDE system manages user identities and how end users can authenticate themselves to XSEDE identities throughout the XSEDE system. A significant requirement is support for “federated identity,” the ability to securely authenticate to XSEDE identities using credentials from other systems (e.g., campuses).

Use case document(s):

- http://hdl.handle.net/2142/45237
- http://hdl.handle.net/2142/88830.

CDP Summary

The functionality in this use case is fully (or x%) supported by operational components listed below.

Gap(s) that we currently plan to address:

- User-defined groups
- Specific credential translations

Gap(s) that will not be addressed at this time:

- Disabling one’s own identity
- Verification of quality attributes

Time and effort summary:

- Approximately five weeks of total effort performed by XUP and Globus teams

Functionality Gaps

1. User-defined groups (suggested priority: high)

Steps 6, 7, 8, and 9 of CAN-9 describe the ability for users to define their own groups of XSEDE users that can then be used to customize access to other XSEDE services. (For example, an XSEDE user may create a group whose membership controls access to specific files in his/her account on a particular XSEDE SP resource.)

Plans: XCI plans to add all of the group functions in the first XSEDE-2 project year (most likely during 2016).

- Integrate Globus user-defined group management into XUP (1 month effort performed by the XUP team and perhaps 1 week effort by Globus team)
- Verify that the WS-Trust STS service properly obtains and encodes group credentials (performed by UVa team prior to end of XSEDE1)

2. Disabling one's own identity (suggested priority: none)

Step 10 in CAN-9 describes the user disabling his/her XSEDE identity so that it can no longer be used. *There is no plan to address this gap and we don't know of any specific instances in which it is needed by scientific users.*

3. Specific credential translations (suggested priority: medium)

XSEDE currently supports all of the steps in CAN-6 (Authenticate to one or more SP resources, SP services, and XSEDE central services), but it doesn't support all of the credential translations identified in the use case. Specifically, we haven't yet finished an activity to develop and deploy a WS-Trust Secure Token Service (STS) for translating OAuth 2.0 tokens into signed SAML assertions. This translation is used by Genesis II clients to obtain the signed SAML credentials needed to use Genesis II and UNICORE clients and services, including both GFFS and remote job submission. Note that Genesis II clients have a pre-existing workaround that uses XSEDE's Kerberos services instead of the Globus Auth service, which produces a similar result but won't work with the user-defined group features mentioned above.

Plans: This work is underway and should be completed during 2016.

- Develop WS-Trust STS service (performed by UVa team prior to end of XSEDE-1)

4. Verification of quality attributes

Verifying quality attributes requires significant one-time and ongoing testing. XSEDE has decided that the costs of this testing would not bring sufficient benefit. Instead XSEDE will monitor user satisfaction, usage, and available performance metrics and address quality issues when raised by users. *There are no plans to address this verification gap.*

System Components That Support These Use Cases

The following XSEDE system components currently support these two use cases.

(Hypelink the component <Name> to the XCSR Component Description Repository)

Component	Supported Functionality
XSEDE User Portal (XUP)	The front-end user interface to the XSEDE system where end users register with XSEDE, manage their user profile information, and reque allocations to use XSEDE SP resources.
XSEDE Central Database (XCDB)	The repository that stores XSEDE user profile data, including everythi except usernames and passwords (see Kerberos, below), user-define groups (currently unimplemented), and links with non-XSEDE identitie (see Globus Auth, below)
Globus Auth	Provides the authentication service used by end users to login to XUP and obtain an XSEDE OAuth2 token that can be used with other XSEDE services, plus the ability for end users to link their XSEDE identities with non-XSEDE identities (e.g., InCommon campus identities, DOE and other agency identities, etc.)
XSEDE Kerberos	The repository that stores XSEDE usernames and passwords and authenticates XSEDE identities for Globus Auth
XSEDE Single Sign On (SSO) Hub	An SSH service hosted by XSEDE that allows XSEDE end users to login using their XSEDE user identity and connect to XSEDE SP resources (where they are authorized) without entering additional user credentials
XSEDE MyProxy	A service hosted by XSEDE that translates XSEDE username and password (see Kerberos above) into X.509 proxy certificates required by some XSEDE and legacy TeraGrid services
XSEDE WS-Trust STS	**Currently in development** A service hosted by XSEDE that translates XSEDE OAuth2 tokens (user identity, group membership) obtained from Globus Auth and XUP into the signed SAML chains required by XSEDE Genesis II and UNICORE services, including GFFS